

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 335 266 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
13.08.2003 Bulletin 2003/33

(51) Int Cl.7: **G06F 1/00**, H04L 29/06,
H04L 9/32, G06F 17/60

(21) Application number: **03380022.8**

(22) Date of filing: **07.02.2003**

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT SE SI SK TR**
Designated Extension States:
AL LT LV MK RO

(72) Inventors:
• **Garcia Garcia-Doncel, Jesus**
28023- Las Rozas., Madrid (ES)
• **Borrero Ortiz, Santiago**
28028- Madrid (ES)

(30) Priority: **12.02.2002 ES 200200333**

(74) Representative: **Davila Baz, Angel et al**
c/o Clarke, Modet & Co.,
Goya, 11
28001 Madrid (ES)

(71) Applicant: **Vodafone Group PLC**
Newbury, Berkshire RG14 1JX (GB)

(54) **Distribution and management process and system for mobile terminals for use rights associated with a purchased content.**

(57) It permits carrying out the secure distribution and purchase on mobile terminals (2) of use rights files that are associated with a content included in a digital file. To do so, it uses the public and private keys conventionally granted to the devices, and consists of encrypting a random session key by means of the public key of the smart card (11) conventionally included in mo-

bile terminals (2). Furthermore, the use rights file is encrypted with the random session key and it sends the encryptions to the mobile terminal (2) where the random session key is decrypted by means of the private key of the smart card (11), and the rights file is decrypted with the obtained random session key, the correct distribution of the use rights file thus occurring.

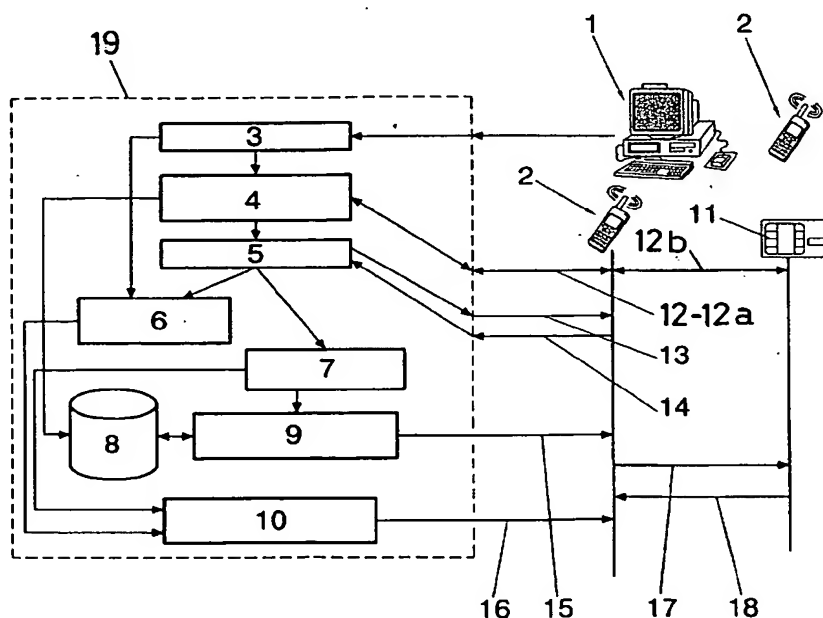


FIG.1

Description**OBJECT OF THE INVENTION**

[0001] The object of the invention concerning us is to provide a process and a device for mobile telephones in the mobile telephone network which permit carrying out the secure distribution and management of use rights associated with a purchased content, such that it prevents piracy and the acquisition of the contents included in digital files comprising different types of information of interest for the user, such as music, video, etc.

BACKGROUND OF THE INVENTION

[0002] The vertiginous development of new technologies and the advance in the processing of digital information has opened a new horizon of possibilities in the business of creation, distribution and sale of contents stored in files containing information of interest for the user (music, video, etc.).

[0003] The popularization of internet has enabled the instantaneous distribution of said contents at the same time that it facilitates the piracy thereof.

[0004] These facts take on special relevance in the music industry with the emergence of the MP3 files format, which enables maximum copying and distribution of music files with a sound fidelity comparable to that of compact discs.

[0005] In the face of this drawback, several groups from the music industry and technological giants came together and created the Safe Digital Music Initiative (SDMI) for Digital Rights Management (DRM) and to protect artists and publishers from the dangers inherent to distribution on the internet, therefore, together with the digital files where the content is stored, a use rights file (voucher) must be purchased, by means of which use rights over said content are defined, it is therefore necessary for the distribution of said use rights files to be carried out securely to those users who have purchased a content, such that only this user can be the person who can access the content of the digital file by making use of the use rights file.

[0006] Technology has continued advancing, permitting the distribution and reproduction of contents to devices that are more and more varied and smaller. In this sense, mobile terminals, which are becoming more and more popular and have greater capabilities, take on special importance.

[0007] There is no process and system in this sector permitting carrying out the secure distribution of use rights files, and which also associates said use rights files with the smart card that the operator provides the user when becoming a subscriber in the operator of the mobile telephone network and which must be included in the mobile terminal so as to permit making calls, such that it permits updating terminals without losing the purchased rights since these are associated with the card

and not with the terminal.

DESCRIPTION OF THE INVENTION

[0008] To solve the aforementioned drawbacks, the invention provides a process and device which permit carrying out the secure distribution of use rights files defining the use of a content included in a digital file (such as music, video, etc.).

[0009] The use rights file can be purchased independently from the digital file storing the content, and the distribution and proper reproduction of said content are not object of the present invention, but rather this is only concerned with proper distribution of the file of use rights that are associated with the digital right.

[0010] To prevent the illegal distribution of contents, encrypting systems have been foreseen consisting of assigning a pair of keys constituted by a public key and a private key to each device, both being mathematically related, and the first one being known by the rest of the devices and the second one known only by the device in question. The private key never travels nor goes outside of said device, such that for sending the contents, these are encrypted with the public key of the device, and they can only be decrypted by means of the private key of said device.

[0011] These keys are assigned by certifying authorities, among which there is a hierarchical relationship. In the case of smart cards, the manufacturers thereof are those who generate the private and public keys, recording the private key in the card and providing the public keys to the network operator buying the cards.

[0012] Then, the process of the invention is characterized in that after receiving a purchase request of a use rights file, it comprises the following phases:

- generating a random session key and the use rights file;
- obtaining the public key of the smart card conventionally associated with the mobile terminal;
- encrypting the random session key with the public key of the smart card;
- encrypting the use rights file with the random session key;
- sending the encryptions carried out to the mobile terminal, where they are received;
- decrypting, in the mobile terminal, the random session key by means of the private key of its smart card; and
- decrypting, in the mobile terminal, the rights file with the random session key obtained in the previous decryption to securely obtain said use rights file since the random session key can only be obtained by the one having the private key of the card of the mobile terminal, upon having been encrypted with the public key of the smart card of the mobile terminal, and therefore it is only permitted to decrypt the use rights file with the delivered session key, which

is also random, in other words, different for each distribution.

[0013] To permit obtaining the public key of the smart cards, said keys are stored in the use files server.

[0014] The process of the invention also foresees that after receiving a purchase request of a use rights file, the cost representing obtaining said use files is sent to the mobile terminal and acceptance is requested, as is conventionally carried out in other processes by means of mobile terminals: pre-payment or by means of deferred payment.

[0015] Furthermore, the process of the invention foresees carrying out a mutual identification process between the mobile terminal and the use rights file server.

[0016] As was previously mentioned, the invention also consists of a system for mobile terminals which permits carrying out the distribution and management of use rights files associated with a purchased content, comprising a server provided with means for receiving a purchase request of a use rights file, means for generating said use rights file. Each mobile terminal is provided with a smart card that is provided with means for storing its own private key, to which a public key is also assigned.

[0017] The novelty of the device of the invention is determined by the fact that the server furthermore comprises means for generating a random session key, means for storing the public key of the smart card of the mobile terminal, means for encrypting the random session key by means of the public key of the mobile terminal, means for encrypting the use rights file by means of the random session key, for sending the encrypted signals to the mobile terminal. These encrypted signals are received by the mobile terminal where the use rights file is decrypted, therefore said mobile terminal has means for decrypting the random session key by means of the private key of the smart card of the mobile terminal such that it obtains the random session key, and means for decrypting the use rights file by means of the obtained random session key, finally obtaining said use rights file.

[0018] In smart cards with cryptographic capacities, the private key is stored in its WIM (Wireless Identification Module) application, foreseen for storing user keys and calculating and verifying digital signatures.

[0019] For ensuring the identity of the parties, the system of the invention foresees the mutual identification between the server and the mobile terminal under any of the established conventional processes for carrying out this function. Therefore, the decryption means are included in the smart card associated with each mobile terminal.

[0020] Furthermore, and in correspondence with the described process, the system of the invention foresees the inclusion of the means conventionally included for verifying whether the user who downloads the use rights file has a balance to pay for the requested content, and

in a negative case, it is not sent.

[0021] In order to aid in better understanding this specification and forming an integral part thereof, a single drawing is attached below which shows the object of the invention with an illustrative and non-limiting character.

BRIEF DESCRIPTION OF THE DRAWING

[0022]

Figure 1.- Shows a functional block diagram of a possible embodiment example of the system of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0023] A description of the invention based on the aforementioned drawing is made below.

[0024] As previously mentioned, the system of the invention is provided for permitting securely carrying out the distribution of use right files associated with a digital file including a content of interest for the user, such as music, video, etc., and which specifies the conditions of use of said content, the content can therefore not be accessed without the use rights file.

[0025] Purchase of the use right file can be completely independent from the purchase of the digital file including the information content and purchased by the user, the distribution and reproduction of said content not being the object of the invention, but rather the object is only focused on the proper distribution of the use rights file, as previously mentioned.

[0026] To carry out the purchase of a use rights file, a request is submitted through any device, such as a personal computer 1 or from a mobile terminal 2, which can be the user's own terminal or any other.

[0027] The user makes the request of the use rights file from a WAP web, SMS or from any other one.

[0028] The system of the invention is materialized in a server 19 which receives the request that is made, it therefore has a reception module 3 of the request made, which in the embodiment example foresees the inclusion of a mutual identification module 4 for mutually identifying the server 19 and the mobile terminal 2 to which the use rights file is sent for ensuring the authenticity of the server and of the mobile terminal.

[0029] The mutual identification process can be any of those conventionally used in the state of the art for different applications, and it could even be unnecessary, as in the case when a request is made from a web page in the zone in which the mutual identification has been previously carried out.

[0030] By way of example, a possible conventional mutual identification manner is described, consisting of sending an encrypted text from the mobile terminal 2 with the public key of the server. At this point, it is important to indicate that in the state of the art, as was

described in the section of the description of the invention, each device is assigned a public and private key, wherein the public key is known by the different devices, and the private one is known only by the device in question, and all this such that the private key of each one of the devices never travels towards the remaining devices, and this key is used for decrypting the information that is encrypted with the public keys of the devices, such that only the messages can be decrypted with the private key of each device. Therefore, in the example concerning us, the server receives the message encrypted with its public key and decrypts the message by means of its private key. Once it is decrypted, it encrypts the message again with the public key of the mobile terminal 2, which, in the specific embodiment example, uses the public key of the smart card 11 that mobile terminals 2 need for being able to make calls, and which is purchased by the user when he/she subscribes to an operator of the mobile telephone network. The public key of the smart card 11 is stored in a database 8 of the server 19 to which the mutual identification module 4 accesses.

[0031] The mobile terminal 2 receives the encrypted message and passes it to the smart card 11 which, by means of its private identification key, decrypts the message and compares the message sent with the one received, such that if they coincide, the authentication of the server 19 is thereby carried out.

[0032] Furthermore, the server 19 has a payment acceptance module 5 which sends the cost of acquiring the use rights file to the user by means of his/her mobile terminal 2, which sends payment acceptance that is detected in the payment acceptance module 5, which activates a use rights file generator 6 which is also connected to the request reception module 3, such that when a use rights file request has been received and payment thereof has been accepted, the use rights file generator generates said file and sends it to a use rights file encryption module 10 with a random session key, the server 19 therefore includes a random session key generator 7 that is connected to the module 10 for carrying out said encryption and sends it 16 to the mobile terminal 2.

[0033] The database 8 is furthermore connected to an encryption module 9 of the random session key with the public key of the smart card 11 of the mobile terminal 2 and sends 15 to the mobile terminal 2 said use rights file encrypted with the random session key.

[0034] The mobile terminal 2 receives the encrypted signals 15, 16 and requests 17 the smart card 11 to decrypt the random session key with its private key, the smart card 11 obtaining the random session key and sends it 18 to the mobile terminal 2, which decrypts the use rights file by means of said random session key since said use rights file was encrypted with the random session key, thus securely obtaining the use rights file.

[0035] In a preferred embodiment of the invention, the WIM (Wireless Identification Module) application is used

which is conventionally loaded in the smart card 11 and which has cryptographic capabilities. This WIM application is conventionally foreseen for storing private and public keys and calculating and verifying digital signatures.

[0036] By way of example, the content could consist of downloading a CD-Rom, and the use rights file could indicate that it is only desired to hear its content three times, such that if, after hearing it three times, hearing it is of interest for the user, new rights could be bought to listen to the contents whenever desired, he/she would therefore have to download another rights file (voucher).

[0037] The user must therefore have a mobile with a player which permits listening to the CD and the corresponding application which permits managing the use rights file according to the system of the invention, as has been described. Since the user has downloaded the content of the CD, he/she can buy the additional rights for this content without needing to download the entire CD again.

Claims

1. A distribution and management process for use rights associated with a purchased content for mobile terminals, wherein a purchase request of a use rights file is received which is associated with the purchase of a content included in a digital file, such that the digital file cannot be used without the use rights file, as the latter specifies the permitted use of the purchased content, the use rights file and the content file can be independently purchased; the process further comprising the use of the private and public keys granted by certifying authorities to the different devices for being able to encrypt and decrypt the signals exchanged between them, the private key being known only by each device and the public key by all of them; **characterized in that** after receiving said request, it comprises:
 - generating a random session key and the use rights file;
 - obtaining the public key of the smart card (11) which is conventionally associated with the mobile terminal (2);
 - encrypting the random session key with the public key of the smart card (11);
 - encrypting the use rights file with the random session key;
 - sending (15, 16) the encryptions carried out to the mobile terminal, the encryptions being received in the mobile terminal (2);
 - decrypting, in the mobile terminal, the random session key by means of the private key of its smart card; and
 - decrypting, in the mobile terminal, the rights file with the random session key obtained in the

previous encryption to obtain said use rights file.

2. A distribution and management process for use rights associated with a purchased content for mobile terminals according to claim 1, **characterized in that** after receiving a purchase request of a use rights file, the cost representing obtaining said use rights file is sent to the mobile terminal and acceptance is requested. 5
3. A distribution and management process for use rights associated with a purchased content for mobile terminals according to claim 2, **characterized in that** the purchase of the content is selectively carried out by means of: pre-payment or deferred payment, after receiving acceptance confirmation. 15
4. A distribution and management process for use rights associated with a purchased content for mobile terminals according to claim 1, **characterized in that** a mutual identification process is carried out between the mobile terminal (2) and the server (19) of the use rights file. 20
5. A distribution and management system for use rights associated with a purchased content for mobile terminals, comprising a server (19) provided with means for receiving a purchase request of a use rights file associated with a content included in a digital file, such that the digital file cannot be used without the use rights file, as the latter specifies the permitted use of the purchased content, being possible to purchase the use rights file and the content independently; the mobile terminals (2) having a smart card (11) provided with means for storing a private key of its own to which a public key is also assigned, said public and private keys being granted by certifying authorities for carrying out the encryption and decryption of the signals exchanged between different devices; **characterized in that** the server (19) comprises means (7) for generating a random session key, means (8) for storing the public key of the smart card (11) of the mobile terminal (2), and means (9) for encrypting the random session key by means of the public key of the smart card (11), means (10) for encrypting the use files by means of the random session key, sending (15, 16) the encrypted signals to the mobile terminal (2), which receives them and includes in its smart card (11) means for decrypting the random session key by means of its private key to obtain said random session key, the mobile terminal (2) comprising means for decrypting the use rights file by means of the obtained random session key; all this so that the mobile terminal (2) obtains said use rights file after having made a purchase request of a use rights file. 25 30 35 40 45 50 55

6. A distribution and management system for use rights associated with a purchased content for mobile terminals according to claim 5, **characterized in that** it comprises means (5) for verifying whether the user who is downloading the use rights file has a balance to pay for the requested content, and in a negative case, it is not sent.

7. A distribution and management system for use rights associated with a purchased content for mobile terminals according to claim 5, **characterized in that** the mutual identification between the server (19) and the mobile terminal (2) is carried out.

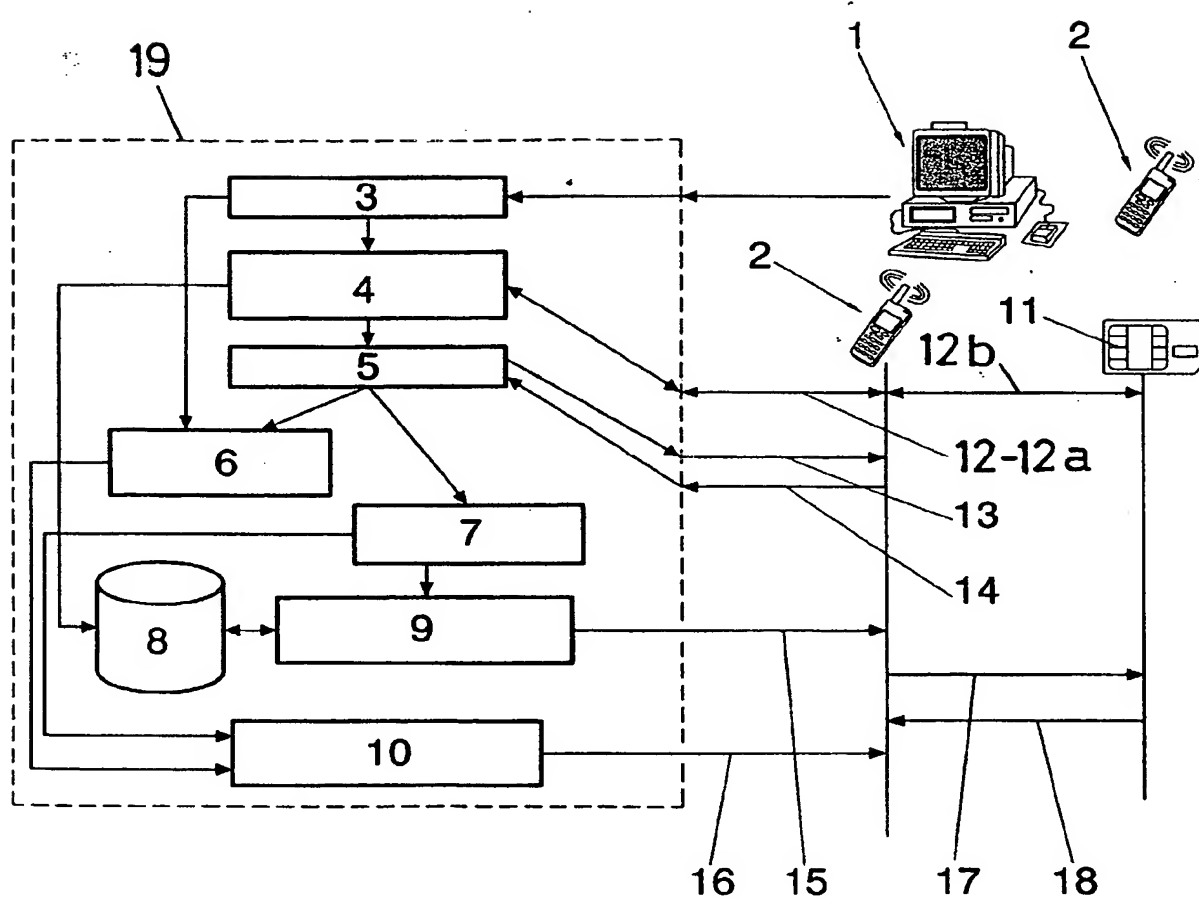


FIG.1



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 38 0022

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	WO 01 98903 A (MINDPORT USA ;FRANSDONK ROBERT W (US)) 27 December 2001 (2001-12-27) * page 1 * * page 4, line 5 - line 24 * * page 5, line 1 - line 16 * * page 9, line 14 - line 38 * * page 11, line 30 - page 12, line 2 * * page 14, line 9 - line 18 * * page 31, line 10 - page 32, line 16 * * page 32, line 34 - page 33, line 2 * * page 33, line 29 - line 36 * * page 42, line 20 - line 30 * * page 47, line 36 - page 48, line 4 * * page 48, line 30 - line 39 * * page 50, line 7 - page 51, line 14 * ---	1-7	G06F1/00 H04L29/06 H04L9/32 G06F17/60
Y	WO 01 63387 A (VISUALGOLD COM INC) 30 August 2001 (2001-08-30) * page 3, line 19 - page 4, line 3 * * page 8, line 27 - page 9, line 37 * ---	1-7	
A	WO 01 41027 A (KOVAC MARIO ;ORSULIC JOSKO (HR); RUNJE DAVOR (HR); UZELAC TOMISLAV) 7 June 2001 (2001-06-07) * page 2, line 10 - page 3, line 31 * * page 5, line 7 - page 7, line 10 * * page 11, line 8 - line 25 * * page 14, line 25 - line 30 * * page 15, line 4 - line 6 * * page 17, line 9 - line 11 * * page 20, line 8 - page 33, line 7 * --- -/--	1-7	G06F H04L
The present search report has been drawn up for all claims			
Place of search MUNICH		Date of completion of the search 14 April 2003	Examiner Apostolescu, R
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03/82 (P04C01)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 38 0022

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	<p>CHOUDHURY A K ET AL: "COPYRIGHT PROTECTION FOR ELECTRONIC PUBLISHING OVER COMPUTER NETWORKS", IEEE NETWORK, IEEE INC. NEW YORK, US, VOL. 9, NR. 3, PAGE(S) 12-20, US XP000505280 ISSN: 0890-8044 * page 15 - page 18 *</p> <p>-----</p>	1-7	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
The present search report has been drawn up for all claims			
Place of search MUNICH		Date of completion of the search 14 April 2003	Examiner Apostolescu, R
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03/02 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 03 38 0022

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-04-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0198903 A	27-12-2001	AU 6985601 A	02-01-2002
		WO 0198903 A1	27-12-2001
WO 0163387 A	30-08-2001	AU 4721301 A	03-09-2001
		WO 0163387 A2	30-08-2001
		US 2002016922 A1	07-02-2002
WO 0141027 A	07-06-2001	AU 1943801 A	12-06-2001
		WO 0141027 A1	07-06-2001

EPO FORM P449

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE LEFT BLANK